## REMARKS

This amendment is filed in response to the FINAL Office Action mailed January 2, 2003. All objections and rejections are respectfully traversed.

Claims 1-49 are pending in the application.

Claims 35-49 were added to better claim the invention

Claims 1, 10, 20, 21, 27, 33, 34 were amended to better the invention.

At paragraph 2-4 of the office action claim 34 was rejected with a citation to MPEP 2106 IV, B, 1(a).

Claim 34 states as follows:

> 34. Electromagnetic signals propagating on a computer network, comprising: said electromagnetic signals carrying instructions for execution on a processor for the practice of the method of claim 10 or claim 27 or claim 40.

At paragraphs 2-4 of the office action claim 34 was rejected under 35 USC 101:

> "because the claimed invention is directed to non-statutory subject matter. Data structures must be embodied on a computer readable medium to be statutory."

The examiner correctly points out that instructions for execution on a processor are patentable subject matter when embodied on a computer readable medium under MPEP 2106

IV, B, 1(a). However, this rejection ignores MPEP 2106 IV, B, 1(c) located at page 2100-14 of the 8th edition of the MPEP. Applicant urges patentability of claim 34 in an argument presented on page 5 of the amendment filed on October 9, 2002 in the above referenced application for United States Patent. To repeat the argument based on paragraph MPEP 2106 IV, B, 1(c), the paragraph states that

> "However, a signal claim directed to a practical application of electromagnetic energy is statutory regardless of its transitory nature."

Applicant respectfully urges that imbedding instructions for execution on a processor in an electromagnetic signal propagating on a computer network meets the requirements of MPEP 2106 IV, B, 1(c), and that claim 34 therefore statutory subject matter.

At paragraph 5 of the office action claims 1 and 10-12 were rejected under 35 U.S.C. 103 (a) as being unpatentable over Hawe et al. US Patent Number 5,070,528 issued December 3, 1991, in view of Chi et al. US Patent Number 5,706,489 issued January 6, 1989.

The present invention, as set out in representative claim 1, comprises in part:

> 1. Apparatus for tightly-coupling hardware data encryption functions with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch, the apparatus comprising:
>
> an encryption execution unit contained within the pipelined processor;
>
> ***an ALU, in response to reading an op-code, enables the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the shared memory; and***
>
> ***a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing.***

Hawe et al., discloses a cryptographic processing unit which connects to a MAC interface so that the cryptographic unit can either receive packets as they are received from a network at the MAC interface, or as they stream to the MAC interface for transmission onto the network. The cryptographic unit may be bypassed by a multiplexer if a packet does not require treatment by the cryptographic unit.

Chi discloses a processor, which uses a parallel instruction execution unit (PIE) so that the processor can offload computationally intense processing to the PIE. The processor executes an instruction which transfers a parallel instruction execution parameter block (PPB) to the PIE. The processor and the PIE facility share RAM storage, and the PIE facility can execute code read from the RAM storage beginning at a location specified in the PPB header. Accordingly, the PIE facility may be used to perform data base record expansion, may perform encryption, data conversion, etc. The PIE performs one sequence of instructions while the processor continues executing another sequence of instructions. (Col. 2, lines 48-52)

Applicant respectfully urges that Applicant's claimed novel

***an ALU, in response to reading an op-code, enables the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the shared memory; and***

***a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing*** is not disclosed by either Hawe or Chi.

In particular, neither Hawe not Chi disclose Applicant's claimed use of ***a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing***.

Hawe either passes data through a bypass or through his encryption unit. Chi has his processor executing a second stream of instructions, while his PIE unit executes a first stream of instructions. Neither Hawe nor Chi disclose Applicant's claimed novel use of a multiplexer to select either the output of an ALU OR the output from the encryption processing unit.

Accordingly, Applicant respectfully urges that Hawe and Chi, taken either singly or in combination, are legally precluded from rendering the present invention obvious under 35 U.S.C. 103(a) because of the absence in both cited patents of Applicant's claimed novel use of ***a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing***.

At paragraph 7 of the office action claims 20-23, 27-29, 33-34 were rejected under 35 U.S.C. 103 (a) as being unpatentable over Hawe and Chi as applied to claim 1, and further in view of Johns-Vano et al. U.S. Patent Number 6,026,490 issued February 15, 2000, and Farrell et al. U.S. Patent Number 5,182,800 issued January 26, 1993.

Johns-Vano discloses a cryptographic processor 100, where the cryptographic processor is controlled by external controller 10 and is provided data from external memory 12. Further, microcode memory 200 stores different sets of microcode which may be transferred over bus 104 to microsequencer 302, depending upon the job that cryptographic processor 100 is requested to perform (column 2 lines 48-54). Accordingly, cryptographic processor 100 may be initialized to perform a variety of requests, as set out in column 3 lines 26-61. Further, the header of a data unit is processed, and depending upon the channel program that directs the microsequencer, the data is copied from the external memory 12 to a specified destination location, after set up of the cryptographic processor has been completed (column 7 lines 35-58).

Farrell discloses a direct memory access controller which provides some pipelining between units attempting to arbitrate for bus 2c. Time constraints on bus 2c are addressed by the Farrell disclosure by using a direct memory access controller memory in conjunction with an additional FIFO memory. The direct memory access controller also contains a tightly

coupled state machine (column 16 lines 60-63), where the state machine 84 (Fig. 8) assists in operation of the direct memory access function.

Applicant respectfully urges that none of the cited patents, Hawe, Chi, Johns-Vano, or Farrell disclose Applicant's claimed novel use of ***a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing***. Johns-Vano discloses a cryptographic processor which operates under the control of his External Controller 10, and so apparently operates asynchronously with respect to whatever controls his External Controller. Farrell discloses an interface to a bus for a device which arbitrates for the bus.

Accordingly, Applicant respectfully urges that Hawe, Chi, Johns-Vano, and Farrell taken either singly or in any combination are legally precluded from rendering the presently claimed invention obvious under 35 U.S.C. 103(a) because of the absence in all cited patents of Applicant's claimed novel

***an ALU, in response to reading an op-code, enables the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the shared memory; and***

***a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing.***

Particularly, there is no mention of Applicants use of ***a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing*** in any of the cited patents, Hawe, Chi, Johns-Vano, or Farrell.

Further, Johns-Vano requires considerable set-up time to begin processing by his cryptographic engine, for example. reading microcode from his microcode memory 200 into his microsequencer 302, etc. In sharp contrast, Applicant's claimed invention shifts execution from the ALU to his encryption execution unit by his ALU executing an op-code as claimed: ***an ALU, in response to reading an op-code, enables the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor*** and so very rapidly shifts from ALU processing to encryption execution unit processing. Johns-Vano is incapable of the rapid encryption and decryption performed by the present invention because of its wasted set up time.

At paragraph 8 of the office action claims 7-9, 13-14, 16-19, 25-27, 30-32 were rejected under 35 U.S.C. 103 (a) as being unpatentable over Hawe, Chi, Narad, Johns-Vano, and Farrell as applied to claims 5, 12, 15, 21, and 28.

Applicant respectively notes that the claims mentioned in paragraph 8 of the Office Action are all dependent claims. All dependent claims are believed to be dependent from allowable independent claims, and accordingly are believed to be in condition for allowance.

Further, Applicant respectively urges that the patents cited hereinabove, each, when taken independently, teach away from the present invention, and therefore cannot be com-

bined under 35 U.S.C. 103 (a) to render to a person of ordinary skill in the art a combination which would be obvious.

Hawe discloses a cryptographic processing unit which connects to a MAC interface so that the cryptographic unit can either receive packets as they are received from a network at the MAC interface, or as they stream to the MAC interface for transmission onto the network. The cryptographic unit may be bypassed by a multiplexer if a packet does not require treatment by the cryptographic unit. A cryptographic header of the packet controls whether the packet is sent through the cryptographic unit, or not.

Accordingly, Hawe teaches away from the present invention in which, according to claim 1, an ALU of a pipelined processor controls whether or not an encryption unit is utilized for a packet being processed by the pipelined processor. The Hawe disclosure teaches control of the cryptographic processor utilizing a header of a packet, where the present novel invention utilizes an ALU of a pipelined processor to determine whether or not to execute special instructions which invoke the encryption execution unit of the present invention.

The Chi patent discloses uses of a parallel instruction execution unit controlled by a command header generated by a processing unit (CPU) 110. The parallel execution unit 120

reads instructions from memory (RAM) storage 130, as directed by entries in the controlling header.

Chi teaches away from the present invention in that Chi teaches that the parallel instruction execution unit must read instructions from a common memory shared with the CPU, while the CPU is executing other instructions. In sharp contrast, the present invention invokes a tightly coupled state machine encryption unit by execution of an op-code by the ALU, and the tightly coupled encryption unit does not arbitrate to read instructions from any memory, especially a memory arbitrated for against the controlling processor.

The Johns-Vano patent discloses a cryptographic engine 100 controlled by an external controller 10, and reading data from an external memory 12 and transferring its output to interface processor 14. Applicant respectfully urges that the architecture of the Johns-Vano disclosure is quite similar to Applicant's Fig 1, which distinguishes prior art from the presently claimed invention, in that both the CPU 110 of Applicant's Fig. 1 and the DES module 160 both compete on bus 150 (Applicant's Fig. 1) for access to memory 120. Applicant's claimed invention has neither his ALU nor his encryption execution unit competing for the shared memory, as the output is selected by Applicant's use of ***a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing***.

Accordingly, applicant respectfully urges that the Johns-Vano disclosure teaches competition on a bus for a shared memory, which the present invention was designed, and claimed, to avoid.

The Farrell patent discloses a direct memory access controller which utilizes a state machine 132 to assist in direct memory access by arbitration for a bus. Farrell uses a number of state machines in his direct memory access design: uses a microchannel state machine 145; uses a FIFO state machine 84 to manage a queue; and, uses a DMAC state machine 103 to assist in direct memory access. As shown in his Fig. 1, Farrell uses the above mentioned state machines in an integrated data link communication controller (IDLC) coupling a network interface 5 to a bus 2c, and providing direct memory access to processor memory RAM 2b.

Accordingly, the Farrell patent teaches the use of state machines in controlling direct memory access between a network interface and a processor and the processor memory. Accordingly, the Farrell disclosure teaches the use of state machines in direct memory access devices and so teaches away from the presently claimed invention in which a tightly coupled state machine is used to perform encryption and decryption calculations. A person of ordinary skill in the art of computer architecture, in following the disclosure of Farrell, would employ a tightly coupled state machine for use in a DMA channel, and nowhere else.

Even further, an analysis under *Graham v. Deere*, 383 U.S. 1, 148 U.S.P.Q. 459, (1966), and cited in MPEP 706.02 (m), comes to the same conclusion, that the claimed invention is novel and non-obvious. The three analytic criteria under *Graham v. Deer* are:

1. Determining the scope and content of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

Further, objective evidence present in the application indicating obviousness or nonobviousness is considered.

Using these analytic criteria, one then makes a legal determination as to whether or not a person of ordinary skill in the pertinent art would have found the claimed invention obvious at the time that the invention was made.

First, the scope and content of the prior art is determined by reference to the cited four patents, Hawe, Chi, Johns-Vano, and Farrell. The scope and content of the prior art is summarized as: Hawe discloses an encryption unit with a straight bypass; Chi discloses a parallel execution unit (PIE) which competes with a controlling processor for a common memory; Johns-Vano discloses a cryptographic processor with an extensive set-up time; and Farrell teaches a direct memory access controller using a plurality of state machines.

2. The differences between the claimed invention and the cited art are, as set out in the claimed novel invention:

***an ALU, in response to reading an op-code, enables the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the shared memory; and***

***a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing.***

Particularly, there is no mention of Applicants use of ***a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing*** in any of the cited patents, Hawe, Chi, Johns-Vano, or Farrell.

Applicant respectfully urges that none of the cited art show ***a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing.***

3. The level of ordinary skill in the art of computer architecture can be ascertained by reference to the cited patents, Hawe, Chi, Johns-Vano, and Farrell. As pointed out hereinabove, each of these cited patents, taken either singly or in any combinatin, teach away from the

presently claimed invention. Accordingly, the level of skill taught by the prior art is totally inadequate to render the presently claimed invention obvious.

Accordingly, it must be concluded that the state of the art before the invention was made is that a parallel execution unit is either bypassed (Hawe), or competes with a controlling processor for a common memory (Chi, Johns-Vano), or that state machines are only used in direct memory access controllers.

Accordingly, the legal conclusion which is required by the application of the *Graham v. Deere* analytic method, is that a person of ordinary skill in the art of the cited art (Hawe, Chi, Johns-Vano, Farrell) could not have found the present invention obvious, because of the absence of the claimed elements of the presently claimed invention in all of the cited art.

All independent claims are believed to be in condition for allowance.

All dependent claims are believed to be dependent from allowable independent claims, and therefore in condition for allowance.

Favorable action is respectfully solicited.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,

A. Sidney Johnston
Reg. No. 29,548
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500

**MARK-UP PAGES FOR THE MARCH 13, 2003, AMENDMENT TO U.S. PATENT APPLICATION SER. NO. 09/216,519**

*The replacement for the FIRST full paragraph of page PAGE resulted from the following changes:*

1. (Twice Amended) Apparatus for tightly-coupling hardware data encryption functions with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch, the apparatus comprising:

an encryption execution unit contained within the pipelined processor; [and]

an ALU, in response to reading an op-code, enables the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the shared memory; and

a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing

[a software and hardware interface that enables the encryption execution unit to efficiently cooperate with resources of the pipelined processor by the pipelined processor executing opcodes to control the encryption execution unit].

10. (Twice Amended) A method for tightly-coupling hardware data encryption functions with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch, the method comprising the steps of:

providing an encryption execution unit within the pipelined processor; [and]

enabling, by an ALU in response to reading an op-code, the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the memory; and

selecting as output the result of processing by the encryption execution unit rather than selecting results from the ALU

[selectively accessing the encryption execution unit through an integrated hardware and software interface of the pipelined processor that allows efficient cooperation between the encryption execution unit and resources of the pipelined processor by the pipelined processor executing opcodes to control the encryption execution unit].

20. (Amended) A programmable processing engine of a network switch comprising:

an input header buffer;

an output header buffer; and

a plurality of processing complex elements symmetrically arrayed into rows and columns that are embedded between the input header buffer and an output header buffer, each processing complex element comprising a microcontroller core having an encryption tightly coupled state machine (TCSM) unit that is selectively invoked [through] in response to the microcontroller reading an op-code; and

a selector to select an output from either the microcontroller OR the TCSM

[an integrated hardware and software interface of the microcontroller core to allow efficient cooperation between the encryption TCSM unit and data path resources of the microcontroller core by the microcontroller executing opcodes to control the TCP].

21. (Amended) A pipelined processor in a network switch, the processor comprising:

an ALU internal to the processor responsive to a first set of opcodes;

an encryption execution unit internal to the processor having an encryption tightly coupled state machine (TCSM) responsive a second set of opcodes, the ALU, in response to an op-code, transferring processing to the encryption execution unit to process [wherein protocol processing operations are performed by the ALU and] encryption operations [are performed by the encryption execution unit]
in response to said second set of opcodes [.] ;

a multiplexer to select output from the ALU OR from the encryption execution unit.

27. (Amended) A method for providing encryption functions within a pipelined processor in a network switch, the method comprising the steps of:

associating a first set of opcodes with an ALU internal to the processor;

associating a second set of opcodes with an encryption execution unit internal to the processor having an encryption tightly coupled state machine (TCSM), wherein protocol processing operations are performed by the ALU and encryption operations are performed by the encryption execution unit in response to said second set of opcodes [.] ; and

transferring by the ALU, in response to an op-code, processing to the encryption execution unit to process encryption operations in response to said second set of opcodes;

selecting output from the ALU OR from the encryption execution unit.

33. (Amended) A computer readable media, comprising: said computer readable media containing instructions for execution in a processor for the practice of the method of claim 10 or claim 27 or claim 40.

34. (Amended) Electromagnetic signals propagating on a computer network, comprising: said electromagnetic signals carrying instructions for execution on a processor for the practice of the method of claim 10 or claim 27 or claim 40.